Cryptography Law of the People's Republic of China

Posted: October-26-2019 Adjust font size:

Order of the President of the People's Republic of China

No. 35

The *Cryptography Law of the People's Republic of China*, adopted at the 14th Meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on October 26, 2019, is hereby promulgated and shall enter into force as of January 1, 2020.

Xi Jinping
President of the People's Republic of China
October 26, 2019

Cryptography Law of the People's Republic of China

(Adopted at the 14th Meeting of the Standing Committee of the Thirteenth National People's Congress on October 26, 2019)

Contents

Chapter I General Provisions

Article 1 This Law is enacted for the purpose of regulating the application and administration of cryptography, promoting the development of cryptography work, ensuring cyber and information security, safeguarding national security and public interests, and protecting the legitimate rights and interests of citizens, legal persons and other organizations.

Article 2 For the purpose of this Law, "cryptography" refers to technologies, products, and services utilized for encryption protection and security authentication on information and the like by using specific transformation methods.

Article 3 Cryptography work shall adhere to a holistic approach to national security, and be in conformity with the principles of unified leadership, hierarchical responsibilities, innovation and development, serving the overall picture, law-based administration, and ensuring security.

Article 4 Cryptography work shall adhere to the leadership of the Communist Party of China. The central leading authority of cryptography work shall uniformly lead nationwide cryptography work, develop national major guidelines and policies for cryptography work, coordinate national significant affairs and tasks concerning cryptography, and promote the rule of law in the national cryptography development.

Article 5 The national cryptography administrative department shall be charge of the nationwide cryptography work. Local cryptography administrative departments at or above the county level shall be charge of cryptography work within their respective administrative areas.

State organs and other entities relating to cryptography work shall be responsible for the cryptography work of their own organs, entities or systems within the scope of their responsibilities.

Article 6 The State shall implement classified administration of cryptography.

Cryptography shall be classified into core cryptography, common cryptography and commercial cryptography.

Article 7 Core cryptography and common cryptography shall be used to secure State secret information. The highest level of information protected by core cryptography shall be top secret, and the highest level of information protected by common cryptography shall be secret.

Core cryptography and common cryptography are State secrets. Cryptography administrative departments shall implement strict and unified administration for core cryptography and common cryptography in accordance

with this Law, other relevant laws, administrative regulations, and State provisions.

Article 8 Commercial cryptography shall be used to protect the information that does not involve anything of State secret.

Citizens, legal persons and other organizations may use commercial cryptography to protect cyber and information security in accordance with law.

Article 9 The State encourages and supports research in and application of cryptography science and technology, protects the intellectual property rights concerning cryptography in accordance with law, and facilitates the progress and innovation in cryptography science and technology.

The State shall strengthen the cultivation and development of cryptography talent teams. The State commends and rewards organizations or individuals that have conducted outstanding contributions to cryptography work in accordance with the relevant State provisions.

Article 10 The State shall take various measures to strengthen public education in cryptography security, incorporate the education of cryptography security into the national education system and public servant education and training system, and enhance the awareness of cryptography security of citizens, legal persons and other organizations.

Article 11 The people's government at or above the county level shall incorporate cryptography work into the corresponding national economic and social development plan, and incorporate required funds into the fiscal budget of the corresponding level.

Article 12 No organization or individual may steal encrypted information or illegally intrude into the cryptography-protected system of others.

No organization or individual may use cryptography to engage in activities endangering national security or public interests or the legitimate rights and interests of others, or other illegal or criminal activities.

Chapter II Core Cryptography and Common Cryptography

Article 13 The State shall strengthen the scientific planning, management and utilization of core cryptography and common cryptography, enhance system building, improve management measures, and enhance cryptography security and protection capability.

Article 14 State secrets that are transmitted in wired or wireless communication and information systems that store or process State secrets shall

be encrypted or authenticated using core cryptography or common cryptography in accordance with relevant laws, administrative regulations, and State provisions.

Article 15 The institutions engaged in scientific research, production, service, testing, equipment, utilizing or destruction of core cryptography and common cryptography (hereinafter collectively referred to as "cryptography working institutions") shall establish and improve the security management system, take strict confidential measures and responsibilities to ensure the security of core cryptography and common cryptography in accordance with relevant laws, administrative regulations, State provisions, and the requirements in core cryptography and common cryptography standards.

Article 16 Cryptography administrative departments shall guide, supervise, and inspect the core cryptography and common cryptography work of cryptography working institutions in accordance with law, and the said institutions shall cooperate.

Article 17 Cryptography administrative departments shall establish core-cryptography-and-common-cryptography-related coordination mechanisms in conjunction with relevant departments based on the needs of work, conducting security surveillance and alert, security risks assessment, information reporting, critical issue consultation, and emergency response to ensure the coordination and efficiency of core cryptography and common cryptography security administration.

If a cryptography working institution detects a core cryptography or common cryptography leak or a major problem or serious risk affecting the security of core cryptography or common cryptography, the institution shall immediately take measures to resolve it and report to the confidentiality administrative department and the cryptography administrative department. The confidentiality administrative department and the cryptography administrative department shall, in conjunction with relevant departments, organize the investigation and response, and guide the relevant cryptography working institution to eliminate security risks in a timely manner.

Article 18 The State shall strengthen the construction of cryptography working institutions to ensure that they fulfill their responsibilities.

The State shall establish the personnel management systems in respect of recruitment, selection, confidentiality, evaluation, training, treatment, award and punishment, exchange and withdrawal, which adapt to the needs of core cryptography and common cryptography work.

Article 19 Cryptography administrative departments may, based on the needs of work and in accordance with relevant State provisions, ask the public security, transport, customs or other relevant departments for privileges such as

inspection exemptions on items and personnel related to core cryptography and common cryptography, and the relevant departments shall cooperate.

Article 20 Cryptography administrative departments and cryptography working institutions shall establish and improve strict supervision and security review mechanisms, oversee staff members as to their compliance with laws and disciplines, and take necessary measures to regularly or irregularly organize security review in accordance with law.

Chapter III Commercial Cryptography

Article 21 The State encourages the research, development, academic exchange, transfer and application of commercial cryptography technology, facilitates a unified, open, competitive, and orderly commercial cryptography market environment, encourages and promotes the development of commercial cryptography industry.

People's governments at various levels and their relevant departments shall follow the non-discrimination principle and provide equal treatment in accordance with law, to all entities, including foreign invested enterprises, which engage in scientific research, production, sale, service, import and export of commercial cryptography (hereinafter collectively referred to as "commercial cryptography entities"). The State encourages foreign investors to cooperate in commercial cryptography technology based on voluntariness and commercial rules. Administrative departments and their staff members shall not force the transfer of commercial cryptography technology by administrative means.

The research, production, sale, service, import and export of commercial cryptography shall not endanger national security, public interests, or the legitimate rights and interests of others.

Article 22 The State establishes and improves the system of commercial cryptography standards.

The standardization administrative department of the State Council and the national cryptography administrative department shall organize the development of national standards and industry standards for commercial cryptography according to their respective responsibilities.

The State supports social organizations and enterprises in using independent innovative technologies to develop association standards or enterprise standards for commercial cryptography that are stricter than relevant technical requirements of national standards or industry standards.

Article 23 The State promotes participation in international standardization activities concerning commercial cryptography and in the development of international standards for commercial cryptography, and advances the conversion between Chinese standards and foreign standards for better application.

The State encourages enterprises, social organizations, educational institutions, scientific research institutes and other organizations to participate in international standardization activities concerning commercial cryptography.

Article 24 Commercial cryptography entities shall, when engaging in activities involving commercial cryptography, comply with the technical requirements prescribed in relevant laws, administrative regulations, mandatory national standards for commercial cryptography and the standards published by such entities themselves.

The State encourages commercial cryptography entities to adopt voluntary national standards and industry standards for commercial cryptography to enhance commercial cryptography protection capability and safeguard the legitimate interests of users.

Article 25 The State facilitates the development of the commercial cryptography testing and certification system, formulates the technical specifications and rules for commercial cryptography testing and certification, and encourages commercial cryptography entities to have their cryptography tested and certified on a voluntary basis to boost their market competitiveness.

Commercial cryptography testing and certification bodies shall obtain relevant qualifications in accordance with law, and conduct commercial cryptography testing and certification in compliance with the laws, administrative regulations, and the technical specifications and rules for commercial cryptography testing and certification.

Commercial cryptography testing and certification bodies shall have the duty to keep confidential any State and commercial secrets learned in the course of commercial cryptography testing and certification.

Article 26 Commercial cryptography products which concern national security, national welfare and people's livelihood, or public interests shall be listed in the catalog of critical network equipment and specialized cyber security products in accordance with law, and be sold or provided for use provided that they have passed the testing and certification conducted by qualified testing and certification bodies. The testing and certification on commercial cryptography products shall be in compliance with relevant provisions of the *Cyber security Law of the People's Republic of China*, and repeated testing and certification

shall be avoided.

Commercial cryptography service using critical network equipment and specialized cyber security products shall pass the certification conducted by a commercial cryptography certification body.

Article 27 Operators of critical information infrastructure shall adopt commercial cryptography to protect such infrastructure if so required by relevant laws, administrative regulations, and State provisions, and shall, conduct application security assessment on commercial cryptography by themselves or by entrusting a commercial cryptography testing body. Commercial cryptography application security assessment shall be coordinated with both critical information infrastructure security testing and assessment system and classified cyber security assessment system to avoid repeated testing and assessment.

Where operators of critical information infrastructure purchase network products and services involving commercial cryptography that may affect national security, such products and services shall be subject to the national security review by the national cyberspace administrative department in conjunction with the national cryptography administrative department and other relevant departments in accordance with the *Cyber Security Law of the People's Republic of China*.

Article 28 The competent department in charge of commerce under the State Council and the national cryptography administrative department shall, in accordance with law, apply import licensing to commercial cryptography which has encryption functionality and concerns national security or public interests, and shall apply export control to commercial cryptography which concerns national security or public interests or which entails international obligations on China. The import licensing list and export control list of commercial cryptography shall be formulated and published by the competent department in charge of commerce under the State Council in conjunction with the national cryptography administrative department and the General Administration of Customs.

Import licensing and export control shall not be applied to commercial cryptography used in mass consumption products.

Article 29 The national cryptography administrative department shall be responsible for the approval of institutions using commercial cryptography technologies to engage in electronic certification service for E-Government activities, and shall, in conjunction with relevant departments, be responsible for the administration of the use of electronic signatures and data messages in administrative activities.

Article 30 Organizations such as commercial cryptography industry associations shall, in accordance with laws, administrative regulations, and their articles of association, provide information, technology, training and other services for commercial cryptography entities, guide and supervise commercial cryptography entities to conduct commercial cryptography activities in accordance with law, improve industry self-discipline and integrity, and promote the healthy development of the industry.

Article 31 Cryptography administrative departments and relevant departments shall establish the mechanism of both in-process and ex-post supervision on commercial cryptography, which combines routine supervision with random inspection, and shall establish a unified information platform for supervision and administration on commercial cryptography, coordinate the in-process and ex-post supervision mechanism and the social credit system, strengthen the self-discipline of commercial cryptography entities and public supervision.

Cryptography administrative departments and other relevant departments, as well as their staff members shall not require commercial cryptography entities or commercial cryptography testing and certification bodies to reveal source code or other cryptography-related proprietary information, and shall strictly keep confidential the trade secrets and individual privacy learned in the course of performing their duty, and shall not disclose or illegally provide such information to others.

Chapter IV Legal Liability

Article 32 In case of a violation of Article 12 of this Law by stealing encrypted information, illegally intruding into the cryptography-protected system of others, or using cryptography to engage in activities endangering national security or public interests or the legitimate rights and interests of others, or other illegal activities, the relevant department shall investigate the legal liability in accordance with the *Cyber Security Law* or other relevant laws or administrative regulations.

Article 33 In case of a violation of Article 14 of this Law and failure in using core cryptography or common cryptography as required, the cryptography administrative department shall give an order of correction or ceasing the illegal activities, and shall issue a warning. Where the circumstances are serious, the cryptography administrative department shall recommend the relevant State organ or entity to impose punishment on the persons in charge who are directly responsible and the other persons who are directly responsible in accordance with law.

Article 34 In case of a core cryptography or common cryptography leak in violation of this Law, the confidentiality administrative department and the cryptography administrative department shall recommend the relevant State organ or entity to impose punishment on the persons in charge who are directly responsible and the other persons who are directly responsible in accordance with law.

In case of a violation of the second paragraph of Article 17 of this Law and failure in taking measures immediately or reporting the situation upon detecting a core cryptography or common cryptography leak or a major problem or serious risk affecting the security of core cryptography or common cryptography in a timely manner, the confidentiality administrative department and the cryptography administrative department shall recommend the relevant State organ or entity to impose punishment on the persons in charge who are directly responsible and the other persons who are directly responsible in accordance with law.

Article 35 Where a commercial cryptography testing or certification body conducts commercial testing and certification in violation of the second or third paragraph of Article 25 of this Law, the market supervision administration shall, in conjunction with the cryptography administrative department, order the said commercial cryptography testing or certification body to make correction or cease the illegal activities, and shall issue a warning and confiscate the illegal gains. Where the amount of illegal gains is RMB 300,000 yuan and above, a fine of not less than one time but not more than three times the amount of illegal gains may be concurrently imposed; where there are no illegal gains or the amount of illegal gains is less than RMB 300,000 yuan, a fine of not less than RMB 100,000 yuan but not more than RMB 300,000 yuan may be concurrently imposed; where the circumstances are serious, the relevant qualifications shall be revoked in accordance with law.

Article 36 Where an untested, uncertified or unqualified commercial cryptography product is sold or provided, or uncertified or unqualified commercial cryptography service is provided in violation of Article 26 of this Law, the market supervision administration shall, in conjunction with the cryptography administrative department, give an order of correction or ceasing the illegal activities, and shall issue a warning and confiscate the illegal products and gains. Where the amount of illegal gains is RMB 100,000 yuan or more, a fine of not less than one time but not more than three times the amount of illegal gains may be concurrently imposed; where there are no illegal gains or the amount of illegal gains is less than RMB 100,000 yuan, a fine of not less than RMB 30,000 yuan but not more than RMB 100,000 yuan may be concurrently imposed.

Article 37 Where an operator of critical information infrastructure, in violation of the first paragraph of Article 27 of this Law, fails to use commercial

cryptography as required, or fails to conduct security assessment on commercial cryptography as required, the cryptography administrative department shall give an order of correction and issue a warning; where the operator refuses to make correction, or the violation has endangered cyber security or caused other results, a fine of not less than RMB 100,000 yuan but not more than RMB 1,000,000 yuan shall be imposed, and a fine of not less than RMB 10,000 yuan but not more than RMB 100,000 yuan shall be imposed upon the persons in charge who are directly responsible.

Where an operator of critical information infrastructure, in violation of the second paragraph of Article 27 of this Law, uses products or services which have not been subjected to or have failed to pass the security review, the relevant administrative department in charge shall order the operator to stop using such products or services, and shall impose a fine of not less than one time but not more than ten times the value of the purchase amount, and a fine of not less than RMB 10,000 yuan but not more than RMB 100,000 yuan upon the persons in charge who are directly responsible and the other persons who are directly responsible.

Article 38 Where the import or export of commercial cryptography is in violation of Article 28 of this Law on import licensing and export control, a punishment shall be imposed in accordance with law by the competent department in charge of commerce under the State Council or the customs.

Article 39 In case of a violation of Article 29 of this Law and engagement in electronic certification service for E-government activities without approval, the cryptography administrative department shall give an order of correction or ceasing the illegal activities, and shall issue a warning and confiscate the illegal products and gains. Where the amount of illegal gains is RMB 300,000 yuan or more, a fine of not less than one time but not more than three times the amount of illegal gains may be concurrently imposed; where there are no illegal gains or the amount of illegal gains is less than RMB 300,000 yuan, a fine of not less than RMB 100,000 yuan but not more than RMB 300,000 yuan may be concurrently imposed.

Article 40 Where, in cryptography work, a staff member of cryptography administrative departments or other relevant departments or entities abuses his or her power, neglect his or her duties or practices favoritism for personal gain, or discloses or illegally provides to others trade secrets or individual privacy he or she has learned in the course of performing his or her duty, the said staff member shall be punished in accordance with law.

Article 41 Where a person or entity violates the provisions of this Law, if a crime is constituted, he or it shall be investigated for criminal responsibility in accordance with law; and shall bear civil liability in accordance with law if damage is caused to others.

Chapter V Supplementary Provisions

Article 42 The national cryptography administrative department shall formulate rules of cryptography administration in accordance with laws and administrative regulations.

Article 43 The Central Military Commission shall formulate measures for cryptography administration of the Chinese People’s Liberation Army and the Chinese People's Armed Police Force in accordance with this Law.

Article 44 This Law shall enter into force as of January1, 2020.